Приложение № 4
к Общим условиям использования электронных документов/ Annex No. 4
to General Terms and Conditions of Use of Electronic Documents

ПОРЯДОК ВЗАИМОДЕЙСТВИЯ СТОРОН ПО ОСУЩЕСТВЛЕНИЮ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ[1]/ PROCEDURE OF INTERACTION OF THE PARTIES IN COURSE OF EXCHANGE OF ELECTRONIC DOCUMENTS[2]

I. При использовании Подсистемы «ИКБ» / With regard to use *ICB* subsystem

1. Обмен Электронными документами/ Exchange of electronic documents

1.1. Для работы в Системе Пользователь Системы использует программно-технические средства, удовлетворяющие требованиям, приведенным в Списке технических и программных средств, необходимых для работы подсистемы «Клиент» (далее – Список).	1.1. For the purpose of working in the System, a System User uses the hardware and software which meet the requirements specified in the List of Hardware and Software necessary for operation of the *Client* subsystem (hereinafter referred to as the List).
1.2. В процессе работы Пользователь Системы выполняет в Системе следующие действия: o Регистрация в Системе – формирование специального ЭД «регистрация», подписанного ЭП Клиента (далее – ЭПК). Работа в Системе возможна только после успешной проверки ЭПК сервером Системы. o Работа с ЭД, исходящими от Клиента, предполагает формирование новых ЭД на основе ЭД, имеющихся в Системе и предусмотренных в Заявлении. Для каждого типа ЭД в Системе имеется соответствующая экранная форма. Для документов «Платежное поручение» возможен импорт в Систему файлов определенного Банком формата. Описание структуры файла импорта имеется на сервере Банка. o Проставление для каждого ЭД одной или нескольких ЭПК. Количество ЭПК для каждого	1.2. In the course of operation, a System User is obliged to perform the following actions within the System: o Registration in the System, which means generation of a special Electronic Document “Registration” signed by the Client’s electronic signature (hereinafter referred to as CES). It is only possible to work in the System following successful authorization of CES by the System server. o Working with ED originated by the Client implies generation of new EDs on the basis of EDs stored in the System and specified in the Application. With regard to each type of ED a relevant display form exists in the System. With regard to *Payment Order* documents it is possible to import in the System files of the format determined by the Bank. A description of the structure of file import is available on the server of the Bank.

[1] Настоящий Порядок определяет порядок взаимодействия Сторон при использовании Клиентом подсистемы «ИКБ» и подсистемы «Прямая интеграция».

[2] This Procedure defines the procedure for interaction between the Parties when the Client uses the subsystem "ICB" and the subsystem "Direct integration".

типа ЭД определено в Заявлении. После подписания ЭД всеми необходимыми ЭПК в соответствии с Заявлением происходит автоматическая пересылка ЭД в Банк для исполнения. ○ Просмотр, печать, сохранение в файл поступивших из Банка ЭД. ○ Выход из Системы.	○ Provision of one or several CESs for each ED. The number of CESs for each type of ED is specified in the Application. Following the signing of ED by all necessary CESs in compliance with the Application, ED is automatically remitted to the Bank for execution. ○ Viewing, printing, storing and filing of EDs which arrive from the Bank. ○ Logging out of the System.
1.3. Процедура обработки ЭД сервером Системы происходит следующим образом: ○ По окончании формирования ЭД Пользователи Системы проставляют ЭПК в количестве, определенном в Заявлении и отправляют ЭД в Банк. ○ Сервер Банка получает ЭД и проверяет корректность всех имеющихся в нем ЭПК. ○ Основанием для принятия Банком ЭД, переданного Клиентом по Системе, является наличие в количестве, установленном в соответствии с Заявлением, и корректность всех ЭПК в ЭД. При положительном результате проверки сервер Банка проставляет в документе отметку о времени приема ЭД и ЭП Банка (далее – ЭПБ), свидетельствующую о получении Банком ЭД, и сохраняет данный ЭД в Системе. При отрицательном результате проверки ЭПК ЭПБ в ЭД не проставляется, Клиент получает сообщение об ошибке средствами Системы. Ключи проверки электронной подписи Банка и копии соответствующих Сертификатов ключей размещаются на сервере системы https://www.bankline.ru. Сертификат Ключа проверки электронной подписи Банка подписывается только уполномоченным представителем Банка. Срок действия Комплекта ключей Банка составляет 5 лет.	1.3. The following procedure for ED processing by the System server is now in place: ○ Following generation of ED by the System User, CESs are fixed in the number specified in the Application, and ED is then sent to the Bank. The server of the Bank receives ED and verifies all CESs contained in ED. Availability of all CESs in the number determined by the Application and authenticity of all CESs in ED constitute the ground for the Bank to accept ED communicated by the Client via the System. In the event of a successful verification, the server of the Bank puts a mark in the document regarding the time of acceptance of ED and ES of the Bank (hereinafter referred to as BES), which confirms the Bank's acceptance of ED. and stores such ED in the System. In the event of a negative result of verification of CES no BES is fixed in ED, and the Client is given an authorization error message via the System. Keys of verification of the Bank's electronic signature and copies of relevant Key Certificates are stored on the System Server at https://www.bankline.ru. The key of authorization of the electronic signature of the Bank is only signed by an authorized representative of the Bank. The set of keys of the Bank is valid for five years.
1.4. Процедуры, описанные в п.1.3 настоящего Порядка, представляют собой единый и неделимый на части процесс получения Банком ЭД, не могут быть выполнены в другой последовательности и рассматриваться независимо друг от друга.	1.4. The procedures described in paragraph 1.3 of this Procedure constitute a single and indivisible process of acceptance of EDs by the Bank and may not be performed in another sequence and may not be viewed separately from each other.

1.5. Документ считается переданным Клиентом в Банк, если он сохранен в архиве исходящих документов Клиента на сервере Банка. Клиент может сохранить любой исходящий документ в файл для ведения собственного архива. Файл должен содержать ЭПК, отметку о времени приема документа Банком и ЭПБ. Файлы с сервера Банка и из архива Клиента могут затем использоваться при процедуре разрешения разногласий между Сторонами.	1.5. A document is deemed to be delivered by the Client to the Bank, if saved in the archive of the Client's documents on the Bank's server. The Client is entitled to save any outgoing document in a file with a view to keep its own archive. The file is to carry CES, a mark about the time of acceptance of the document by the Bank and BES. Files stored on the Bank's server and in the Client's archive may be subsequently used in the course of dispute settlement between the Parties.
1.6. Переданный Клиентом в Банк ЭД в каждый момент времени имеет на сервере Банка определенный статус с отметкой времени его получения. Статус ЭД изменяется Банком. Клиент имеет возможность постоянно получать на сервере Банка информацию об изменении статуса (в том числе о времени его изменения) переданного в Банк ЭД. Сервер Банка присваивает полученным от Клиента ЭД следующие статусы: Рублевые платежные поручения: o получен Банком o документ отправлен на исполнение o Рассчитана комиссия за РКО xx.xx. o Принято или «обработано с ошибкой» с указанием причины, по которой документ отвергнут; o Отправлен на валютный контроль o Включен в рейс для РКЦ o Исполнен Остальные типы документов: o получен Банком o документ отправлен на исполнение o Принят к исполнению или "обработано с ошибкой" с указанием причины, по которой документ отвергнут; o Реестр к росписи o Реестр расписан или частично расписан в случае частичной росписи o Сообщение отправлено в филиал o Документ получен сотрудником валютного контроля. Стороны признают, что надлежащим уведомлением Банком Клиента о приеме к исполнению ЭД Клиента будет являться	1.6. ED handed over by the Client to the Bank at each point of time has a relevant status on the Bank's server with a note of time of its receipt. ED status may be modified by the Bank. The Client enjoys an opportunity to receive on a continuous basis information from the Bank's server concerning status modification (including the time of its modification) of the electronic document handed over to the Bank. The server of the Bank assigns the following statuses to electronic documents received from the Client: Payment order in rubles: o Accepted by the Bank o Document sent for execution o Cash and settlement service fee charged in the amount of xx.xx. o Accepted or processed with error, with indication of the reason underlying rejection of the document; o Sent to foreign exchange control o Put on the dispatch list for delivery to cash settlement center o Settled Other types of documents: o Received by the Bank o Document sent for execution o Accepted for execution or processed with error, with indication of the reason underlying rejection of the document; o Register breakdown o Register broken down or partially broken down in the event of partial breakdown o Message sent to subsidiary o Document accepted by foreign-exchange control officer.

присвоение Банком ЭД Клиента статуса “документ отправлен на исполнение”, а при работе в Депозитарном модуле Системы - получение Клиентом документа типа «Статус обработки распоряжения/запроса», в котором указано, что статус обработки соответствующего ЭД Клиента «Принято к исполнению». Банк информирует Клиента об исполнении каждого ЭД Клиента путем направления Клиенту соответствующего уведомления посредством Системы. Примечание: Перечень и описание статусов ЭД, присваиваемых сервером Банка в Депозитарном модуле Системы, приведены в руководстве пользователя Депозитарного модуля Системы.	The Parties acknowledge that assigning of the Client’s *Document Sent for Execution* status will constitute the Bank’s appropriate notification of the Client about acceptance of the Client’s document for execution, and with regard to working in the Depository Module of the System – receipt by the Client of the document with the *Status of Processing of an Order/Request* type which specifies that the status of processing of a relevant ED of the Client is *Accepted for Execution*. The Bank notifies the Client about execution of every ED of the Client by forwarding to the Client a relevant notification via the System. Note: The list and description of statuses of EDs assigned by the Bank’s server in the Depository Module of the System are given in the User Manual in the Depository Module of the System.
1.7. При формировании ЭД для Клиента Банк проставляет в нем ЭПБ. ЭД считается переданным Банком Клиенту, если он подписан ЭПБ и выложен на сервер Банка, то есть имеется в списке входящих ЭД Клиента на сервере Банка. Клиент может сохранить любой входящий документ в файл для ведения собственного архива. Файлы архива могут затем использоваться при разрешении разногласий.	1.7. When generating ED for the Client, the Bank will fix its electronic signature in such document. ED is deemed transmitted to the Client by the Bank, if signed by BES and placed on the Bank’s server, i.e. such ED is on the list of the Client’s incoming electronic documents on the Bank’s server. The Client may save any incoming document in a file for maintaining its own archive. Archive files may consequently be used in the course of dispute settlement.
1.8. Банк фиксирует электронные архивы полученных от Клиента ЭД, содержащих ЭПК и ЭПБ, и доставленных Клиенту ЭД, содержащих ЭПБ, и хранит их способом, обеспечивающим Клиенту доступ к данным ЭД на сервере Банка.	1.8. The Bank will record the electronic archives of electronic documents obtained from the Client, which carry CESs and BESs and EDs delivered to the Client which carry CESs and kept in a mode which provides the Client with access to EDs with BES on the Bank’s server.
1.9. Клиент с помощью программы проверки ЭП CryptoManager.exe, установленной на Персональном компьютере, имеет возможность в любой момент времени проверить ЭПБ и ЭПК любого файла архива. Вышеуказанная программа проверки ЭП позволяет выполнять проверку типов ЭП (раздел 3 настоящего Порядка), разрешенных для использования в Системе.	1.9. Based on the use of *CryptoManager.exe* verification program installed in PC, the Client may at any point of time verify BES and CES fixed in any archive file. The above ES verification software provides for verifying ES types (section 3 of this Procedure), allowed for use in the System.
1.10. Программу проверки ЭП CryptoManager.exe можно получить у фирмы-	1.10. *CryptoManager.exe* ES verification software may be obtained from the manufacturer of

разработчика Системы – ЗАО «ИНИСТ» (Лицензия ФСБ России № 12818Н от 16.04.2013), зарегистрированной по адресу 119334, г. Москва, 5-ый Донской проезд, д.15, стр.2.	the System CJSC INIST (License issued by the Federal Security Service (FSB) of Russia No.12818N on April 16, 2013) registered at 119334, Moscow, 5th Donskoy proezd, 15, building 2.

2. Порядок получения, замены и хранения ключей/ Procedure for receiving, replacing and storaging of keys

2.1. Для Комплектов ключей, сгенерированных для работы на Персональном компьютере Клиентами, относящимися к корпоративному сегменту:	2.1. With regard to sets of keys generated for operation of PCs by business segment Clients:
2.1.1. Клиент может генерировать Комплекты ключей своих Пользователей Системы согласно Заявлению с помощью программных средств, предоставленных Банком, на USB-токенах или иных носителях информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.) с использованием своих технических средств.	2.1.1. The Client may generate sets of keys for its System Users on the basis of an Application with use of the software provided by the Bank, on USB tokens and other storage media (hard discs, removable media (flash memory, external hard discs), etc.) on the basis of its own technical facilities.
2.1.2. Первый Ключ проверки электронной подписи каждого Пользователя Системы регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе.	2.1.2. The first Electronic Signature verification key of each System User shall be registered by the Bank on the basis of the Key Certificate signed by the Parties and executed in hard copy.
2.1.3. Второй и последующий Ключи проверки электронной подписи регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе, или на основании электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, являющегося единоличным исполнительным органом Клиента и направленного в Банк с использованием Системы. При этом, Банк вправе запрашивать, а Клиент обязан по запросу Банка предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия Пользователя, в том числе являющимися единоличным исполнительным органом.	2.1.3. The second and subsequent Electronic Signature verification keys shall be registered by the Bank on the basis of the Key Certificate signed by the Parties executed in hard copy, or on the basis of a request for release of the Key Certificate to be signed by the System User's electronic signature effective at the date of signing, which System User acts as a sole executive body of the Client, and thereafter to be sent to the Bank via the System. In such case the Bank shall be entitled to request, and the Client shall be obliged pursuant to such request to submit documents to the Bank (in the form of the originals or duly certified copies thereof), which confirm the powers of the User, including those of the sole executive body.

2.1.4. Срок действия Комплекта ключей указывается в Сертификате ключа. Срок действия Комплекта ключей не может превышать срок действия полномочий Пользователя Системы в соответствии с документами, подтверждающими его полномочия. В случае если исходя из представленных Клиентом документов не представляется возможным установить срок действия полномочий Пользователя Системы, срок действия Комплекта ключей не может превышать трех лет. До истечения установленного срока Клиент обязан инициировать процедуру смены Комплектов ключей. По заявлению Клиента, направленному в Банк в произвольной форме средствами Системы до окончания срока действия Комплекта ключей, его действие может быть продлено на срок не более 3 (трех) месяцев. По инициативе Клиента Комплект ключей может быть заменен в любой момент его действия. Каждый новый Сертификат ключа, подписанный Сторонами, автоматически отменяет действие Сертификата ключа данного Пользователя Системы, выпущенного ранее.	2.1.4. The period of validity of the set of keys is specified in the Key Certificate. The said period may not exceed the term of authority of a System User pursuant to the documents which confirm his/her authority. In cases where based on the documents provided by the Client it is deemed impossible to determine the term of effect of the System User's authority, the period of validity of ф set of keys may not exceed three years. Prior to expiration of the established period, the Client is obliged to initiate the procedure of replacement of sets of keys. Based on the Client's application submitted to the Bank in a free format via the System facilities prior to expiration of the term of validity of a set of keys its effect may be extended for a term not exceeding 3 (three) months. At the initiative of the Client, a set of keys may be replaced at any point of time of its effect. Each new key certificate signed by the Parties will automatically supersede the effect of the previously issued key certificate of a particular System User.
2.1.5. Оформленные со стороны Банка Сертификаты ключей Клиента вручаются УПК либо направляются Клиенту посредством почтовой связи по адресу Клиента, указанному в Договоре. Сертификаты ключей должны храниться у каждой из Сторон не менее пяти лет после окончания их срока действия.	2.1.5. The Client's key certificates generated by the Bank are to be handed to ARC, or mailed to the Client's address specified in the Agreement. Key certificates are to be kept by each of the Parties for not less than five years following expiration of the term of their validity.
2.1.6. При поступлении электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, Банк направляет Клиенту с использованием Системы Сертификат ключа, подписанный электронной подписью уполномоченного представителя Банка. При этом Клиент вправе обратиться в Банк с целью получения копии Сертификате ключа на бумажном носителе, заверенной Банком как удостоверяющим центром.	2.1.6. Upon arrival of an electronic request for issuance of a Key Certificate signed by the System User's Electronic Signature effective at the date of signing, the Bank shall send via the System the Key Certificate signed by the electronic signature of an authorized representative of the Bank. In such case the Client is entitled to apply to the Bank for a hard copy of the Key Certificate certified by the Bank as a certification center.
2.1.7. В случае информирования Банком Клиента в Системе о необходимости осуществить замену USB-токена соответствующего типа, Клиент обязан осуществить замену USB-токена. С момента информирования Банком Клиента в	2.1.7. In case the Bank notifies the Client via the System about the need to replace a USB token of a relevant type, the Client is obliged to replace the USB token. As from the date of such notification, no

Системе о необходимости осуществить замену USB-токена, генерация Комплектов ключей с помощью USB-токена, подлежащего замене, не осуществляется.	key sets may be generated with the help of the USB token subject to replacement.
2.2. Для Комплектов ключей, сгенерированных для работы на Персональном компьютере Клиентами, относящимися к сегменту предпринимателей:	2.2. With regard to the key sets generated for operation of PCs by business segment Clients:
2.2.1. Клиент может генерировать Комплекты ключей своих Пользователей Системы согласно Заявлению с помощью программных средств, предоставленных Банком, на USB-токенах или иных носителях информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.) с использованием своих технических средств.	2.2.1. The Client may generate sets of keys for its System Users based on the Application with the help of the software provided by the Bank, on USB tokens or other information media (hard disks, removable media (flash disks, external hard disks), etc.) with use of its own technical facilities.
2.2.2. Первый Ключ проверки электронной подписи каждого Пользователя Системы регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе.	2.2.2. The first ES verification key of each System User is to be registered by the Bank on the basis of the key certificate signed by the Parties and executed in a hard copy.
2.2.3. Второй и последующий Ключи проверки электронной подписи регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе, или на основании электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, и направленного в Банк с использованием Системы. Указанный запрос также может быть подписан простой электронной подписью Пользователя Системы, сформированной на основании предъявленного клиентом SMS-кода, ранее направленного Банком на номер телефона данного Пользователя Системы, указанный в Заявлении и/или предоставленный Банку Пользователем Системы в процессе обслуживания в Системе. Пользователь Системы должен обладать полномочиями на направление в Банк соответствующего электронного запроса. При использовании Клиентом Системы при наличии открытого расчетного счета подпись такого Пользователя должна быть включена в карточку с образцами подписей и оттиска печатей,	2.2.3. The second and subsequent ES verification keys are to be registered by the Bank on the basis of the key certificate signed by the Parties and executed in a hard copy, or on the basis of an electronic application for issuance of a key certificate signed by an electronic signature of the System User effective as at the date of signing by the System Users of ES and forwarded to the Bank via the System. The above application may also be signed by a System User's basic electronic signature generated on the basis of the SMS code previously sent by the Bank to the telephone number of such System User specified in the Application and/or provided by the System User to the Bank in the course of service in the System. A System User is to be authorized to send to the Bank a relevant electronic request. In case where the Client uses the System in in conjunction with a current account, the signature of such User is be recorded in the banking sample signatures and seal card which are attached to the Client's account serviced within the framework of the Agreement, if such card is in place. In such case the Bank has the right to request, and the Client is obliged following the Bank's request, to submit to the Bank the documents (in the form of originals or duly certified copies), which confirm the

действующей к счету Клиента, обслуживаемому в рамках Договора, в случае ее оформления. При этом, Банк вправе запрашивать, а Клиент обязан по запросу Банка предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия Пользователя по направлению в Банк электронного запроса на выдачу Сертификата ключа.	User's authority to forward to the Bank an electronic request for issuance of a key certificate.
2.2.4. Срок действия Комплекта ключей определяется Банком и указывается в Сертификате ключа. Срок действия Комплекта ключей не может превышать срок действия полномочий Пользователя Системы в соответствии с документами, подтверждающими его полномочия. В случае, если исходя из представленных Клиентом документов не представляется возможным установить срок действия полномочий Пользователя Системы, срок действия Комплекта ключей не может превышать трех лет. До истечения установленного срока действия Комплекта ключей Клиент обязан инициировать процедуру смены Комплектов ключей. При этом, до окончания срока действия Комплекта ключей Клиент может продлить его действие на срок не более 3 (трех) месяцев, направив в Банк заявление посредствами Системы. По инициативе Клиента Комплект ключей может быть заменен в любой момент его действия. Каждый новый Сертификат ключа, подписанный Банком, автоматически отменяет действие Сертификата ключа данного Пользователя Системы, выпущенного ранее.	2.2.4. The term of validity of a set of keys is to be determined by the Bank and specified in the key certificate. The said term may not exceed the period of validity of the authority of a System User in accordance with the documents which confirm the User's authority. In cases where it is deemed impossible to identify the term of validity of the System User's authority, the term of effect of a set of keys may not exceed three years. Prior to expiration of the established term of a set of keys the Client is obliged to initiate the procedure of substitution of a set of keys. In such case, prior to expiration of the term of validity of a set of keys the Client may extend the term of not more than 3 (three) months by forwarding to the Bank a relevant application via the System. At the initiative of the Client, a set of keys may be replaced at any point of time of its effect. Each new key certificate signed by the Bank automatically supersedes the effect of the previously issued key certificate of a particur System User.
2.2.5. Оформленные со стороны Банка Сертификаты ключей Клиента на бумажных носителях вручаются уполномоченному представителю Клиента либо направляются Клиенту посредством почтовой связи по адресу Клиента, указанному в Договоре. Сертификаты ключей должны храниться у каждой из Сторон не менее пяти лет после окончания их срока действия.	2.2.5. The Client's key certificates executed by the Bank in hard copies are to be handed to an authorized representative of the Client, or mailed to the Client's address specified in the Agreement. The Parties are obliged to keep key certificates for not less than five years following expiration of their validity.
2.2.6. При поступлении электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы, Банк направляет Клиенту с	2.2.6. Upon arrival of an electronic application for issuance of a key certificate signed by the System User's electronic signature effective as at the date of signing, the Bank is to send to the Client via the System a key certificate with an electronic

использованием Системы Сертификат ключа, подписанный электронной подписью уполномоченного представителя Банка. При этом Клиент вправе обратиться в Банк с целью получения копии Сертификата ключа на бумажном носителе, заверенной Банком как удостоверяющим центром.	signature of an authorized representative of the Bank. In such case the Client has the right to request to the Bank to issue a hard copy of the key certificate certified by the Bank acting as a certification authority.
2.2.7. В случае информирования Банком Клиента в Системе о прекращении действия имеющегося у Клиента USB-токена соответствующего типа, Клиент должен осуществить процедуру смены Комплектов ключей своих Пользователей Системы: • путем генерирования Комплектов ключей своих Пользователей Системы на иных носителях информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.) с использованием своих технических средств, либо • путем осуществления замены USB-токена, посредством обращения в подразделение Банка.	2.2.7. In the event that the Client is notified by the Bank about termination of the effect of the Client's USB token of a relevant type, the Client is obliged to perform the procedure of replacement of the sets of keys of its System Users: • By way of generating sets of keys of its System Users on other media (hard disks, removable media (flash disks, external hard disks), etc.) with use of its own technical facilities, or • By way of replacing a USB token following a relevant request to the Bank.
2.3. Для Комплекта ключей, сгенерированного посредством Мобильного приложения:	2.3. With regard to the set of keys generated with the help of a mobile application:
2.3.1. Пользователь вправе генерировать Комплект ключей для Мобильного приложения с помощью программных средств, предоставленных Банком, при наличии действующего Комплекта ключей, сгенерированного для работы на Персональном компьютере.	2.3.1. The User has the right to generate a set of keys for a mobile application with the help of the software provided by the Bank in the existence of an effective set of keys generated for working on PC.
2.3.2. Срок действия Комплекта ключей указывается в Сертификате ключа. Срок действия Комплекта ключей, сгенерированного посредством Мобильного приложения, не может превышать срок действия Комплекта ключей Пользователя, сгенерированного для работы на Персональном компьютере. До истечения установленного срока Клиент обязан инициировать процедуру смены Комплектов ключей. Каждый новый Сертификат ключа, подписанный Сторонами, автоматически отменяет действие Сертификата ключа данного Пользователя Системы, выпущенного ранее.	2.3.2. The term of validity of a set of keys is specified in the key certificate. The term of validity of a set of keys generated with the use of a mobile application may not exceed the term of validity of the User's set of keys generated for working on PC. Prior to expiration of the established period, the Client is obliged to initiate the procedure of replacement of a set of keys. Each new key certificate signed by the Parties will automatically supersede the effect of the previously issued key certificate of such System User.
2.3.3. Статус ЭП Пользователя Системы, сгенерированной посредством Комплекта ключей	2.3.3. The status of ES of a System User generated with the use of a set of keys for a mobile

для Мобильного приложения, соответствует Статусу ЭП Пользователя Системы, указанному в Заявлении, при генерации Комплекта ключей на USB-токенах или иных носителях информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.)	application corresponds to the status of the electronic signature of a System User specified in the Application upon generation of a set of keys on USB tokens or other media (hard disks, removable media (flash disks, external hard disks), etc.).
2.3.4. Обязательная замена Комплекта ключей проводится в следующих случаях: • истек срок действия Комплекта ключей; • произошла Компрометация ключей.	2.3.4. It is required to replace a set of keys in the following cases: • The term of validity of a set of keys has expired; • The keys have been compromised.
2.4. В случае лишения Клиентом Пользователя Системы права подписывать ЭП ЭД соответствующие Комплекты ключей выводятся из действия на основании письменного заявления Клиента или ЭД свободного формата, направленного в Банк посредством Системы и подписанного уполномоченным лицом Клиента.	2.4. In case the Client denies a System User the right to sign an electronic document with ES the relevant key sets are be disabled pursuant to a written application of the Client or an electronic document of a free format sent to the Bank via the System and signed by an authorized representative of the Client.
2.5. Банк вправе аннулировать Сертификат ключа в следующих случаях: • не подтверждено, что владелец Сертификата ключа владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате; • установлено, что содержащийся в Сертификате ключ проверки ЭП уже содержится в ином ранее созданном Сертификате ключа; • вступило в силу решение суда, которым, в частности, установлено, что Сертификат ключа содержит недостоверную информацию. Информация о прекращении действия Сертификата ключа вносится Банком в соответствующий реестр сертификатов в срок, установленный действующим законодательством Российской Федерации.	2.5. The Bank has the right to revoke a key certificate in the following cases: • There is no confirmation that a certificate holder possesses the ES key which corresponds to the ES verification key specified in such certificate; • It is established that the ES verification key specified in the certificate already exists in another previously generated key certificate; • A court decision came into effect, which in particular established that the key certificate contains unreliable information. The Bank records information concerning revocation of a key certificate in a relevant certificate register within the term established by the applicable law of the Russian Federation.

3. Обеспечение безопасности процедуры обмена документами/ Maintenance of security of document exchange procedure

3.1. Безопасность обмена ЭД достигается за счет применения следующих средств:	3.1. Security of ED exchange is ensured via use of the following facilities:
3.1.1. Для Персонального компьютера:	3.1.1. With regard to personal computers:

Средство криптографической защиты информации (СКЗИ) на базе Программного комплекса «Бикрипт 5.0.» (вариант исполнения 2), разработанного ООО Фирма «ИнфоКрипт» (сертификат соответствия ФСБ РФ СФ/114-3535 от 12.12.2018 г.). Клиент имеет право вместо USB-токенов использовать для хранения Ключа электронной подписи иные носители информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.). Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации за исключением USB-токенов. Использованием СКЗИ «Криптотокен 2 ЭП» в составе USB-токенов JaCarta-2 ГОСТ, разработанных АО «Аладдин Р.Д.» (сертификат соответствия ФСБ России № СФ/124 – 3956 от 17.11.2020 г.). Ключ электронной подписи никогда не покидает внутренней защищенной памяти USB-токена. Генерация и хранение Ключа электронной подписи, а также подписание документов производится во внутренней защищенной памяти USB-токена. Доступ к Ключу электронной подписи осуществляется с использованием пароля. Клиент имеет право вместо USB-токенов использовать для хранения Ключа электронной подписи иные носители информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.). Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации за исключением USB-токенов. Шифрования данных в телекоммуникационных каналах с использованием СКЗИ КриптоПро CSP версии 4.0 и выше. Для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется	Cryptographic information protection facilities (CIPFs) on the basis of the software solution Bicrypt 5.0. (version 2) developed by InfoCrypt LLC (certificate of conformity issued by the Federal Security Service (FSB) of the Russian Federation (FSB) No. SF/114-3535 of December 12, 2018). For the purpose of safe-keeping electronic signature keys, a Client is entitled to use information media instead of USB tokens (hard discs, removable media (flash memory, external hard discs), etc.). The Client is notified by the Bank that utilization of other information media in lieu of USB tokens significantly reduces the level of security in the course of ED exchange, and therefore is fully aware of resulting risks. The Bank recommends to abstain from using any information media other than USB tokens. Utilization of CIPF Cryptotoken 2 ES in conjunction with USB tokens JaCarta-2 GOST developed by JSC Aladdin R.D. (certificate of conformity issued by the Federal Security Service (FSB) of the Russian Federation (FSB) No. SF/124 – 3956 of November 17, 2020). An electronic signature key is never detached from the internal protected memory of a USB token. ES keys are generated and signing of documents is performed inside the internal protected memory of a USB token. Access to ES key is obtained with use of a password. A Client has the right to use other information media in lieu of USB tokens when safe-keeping ES keys (hard discs, removable media (flash memory, external hard discs), etc.). The Client is notified by the Bank that utilization of other information media in lieu of USB token seriously affects the level of security in the course of ED exchange, and is fully aware of resulting risks. The Bank recommends to abstain from using any information media other than USB tokens. Data encryption in telecommunication channels with use of CIPF CryptoPro CSP of version 4.0 and higher. With a view to protect data from unauthorized access in telecommunication channels, protocol Transport Layer Security (TLS v. 1.2, RFC 2246 and above 3) is recommended for use. Certification of appurtenance of the System server of PJSC ROSBANK with the help of a certificate issued to PJSC ROSBANK by the Certification Authority of CRYPTO-PRO LLC.

[3] It is recommended to use version *TLS v.1.2*.

протокол Transport Layer Security (TLS v. 1.2, RFC 2246 и выше2). Удостоверения принадлежности сервера Системы ПАО РОСБАНК с помощью сертификата, выданного ПАО РОСБАНК аккредитованным Удостоверяющим центром ООО «КРИПТО-ПРО».	
3.1.2. Для Мобильного приложения: Средства криптографической защиты информации с использованием алгоритма RSA для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол Transport Layer Security (TLS v.1.2, RFC 2246), применяются криптографические международные алгоритмы шифрования RSA (3072 bit), обмена ключей по алгоритму Диффи-Хеллмана, хэширования в соответствии с SHA 512. Симметричное шифрование AES с длиной ключа 256 bit., генерация и хранение Ключа электронной подписи, а также подписание ЭД производится во внутренней защищенной памяти Мобильного устройства. Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации, предназначенных для генерации и хранения ключа ЭП, за исключением USB-токенов.	3.1.2. With regard to mobile apps: Cryptographic information protection facilities with use of RSA algorithm for the purpose of protecting data from unauthorized access in telecommunication channels protocol Transport Layer Security (TLS v.1.2, RFC 2246) is used, as well as international cryptographic encryption algorithms RSA (3072 bit), exchange of keys on the basis of the Diffie-Hellman algorithm and hashing in accordance with SHA 512. AES symmetric encryption with the key length of 256 bit., generation and safe-keeping of ES keys, as well as signing with the help of ES are performed in the internal protected memory a mobile device. The Client is notified by the Bank that utilization of other information media in lieu of USB token seriously affects the level of security in the course of ED exchange, and is fully aware of resulting risks. The Bank recommends to abstain from using any information media for generating and safe-keeping ES keys other than USB tokens.
3.2. Клиенту рекомендуется обеспечить комплекс организационно-технических мер, направленных на выполнение следующих требований безопасности:	3.2. The Client is recommended to arrange a comprehensive set of organizational and technical measures designed to meet the following security requirements:
3.2.1. Для работы на Персональном компьютере: Организовать выделенный компьютер подсистемы «Клиент», предназначенный исключительно для работы с Банком; Генерацию и хранение ключевой информации, а также подписание документов производить с использованием USB-токенов JaCarta -2 ГОСТ;	3.2.1. With regard to PC operation: To allocate a dedicated PC of the Client subsystem intended exclusively for communicating with the Bank; Generation and safe-keeping of key information, as well as signing of documents shall only be performed with use of USB tokens JaCarta -2 GOST;

[2] Рекомендуется использовать версию TLS v.1.2.

В случае генерации Клиентом, относящимся к сегменту предпринимателей, Ключей электронной подписи своих Пользователей на носители, отличные от USB-токенов, осуществлять эксплуатацию рабочего места и обеспечение его безопасности организационными и техническими мерами в соответствии с требованиями эксплуатационной документацией для СКЗИ «Бикрипт 5.0» для класса КС1: «Средство криптографической защиты информации «Бикрипт 5.0». Правила пользования» (ИНФК.11485466.4012.027.31). Данный документ размещен на официальном сайте Банка в сети Интернет по адресу http://www.rosbank.ru. Ввести ограничение сетевого взаимодействия компьютера подсистемы «Клиент» только с необходимым доверенным перечнем IP-адресов; Проверять, что установлено защищенное TLS-соединение с официальным ресурсом сервиса https://www.bankline.ru. Средствами подсистемы «Клиент» закрепить за Пользователями Системы IP-адрес/список IP-адресов компьютеров подсистемы «Клиент» в целях обеспечения контроля на стороне Банка; Обеспечить на выделенном компьютере наличие средств защиты от вредоносного программного обеспечения, их работоспособность и регулярное обновление; Исключить на выделенном компьютере открытие писем с вложениями, полученными от неизвестных или недоверенных источников; Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы; Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы; Исключить использование средств удаленного администрирования; Обеспечить применение лицензионного межсетевого экрана (допускается использование персонального межсетевого экрана; Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности	In case a business segment Client generates ES keys for its Users on information media other than USB tokens, it is necessary to operate workstations and ensure their security with reliance on organizational and technical measures in compliance with the operating document requirements for CIPF Bicrypt 5.0 for class KS1: Cryptographic information protection facility Bicrypt 5.0. Directions for Use (INFK.11485466.4012.027.31). The said document is available on the official web-site of the Bank at http://www.rosbank.ru. To introduce restriction of network interconnection of the Client subsystem PC exclusively with the required trusted list of IP addresses; To verify whether a TLS protected connection with the official resource https://www.bankline.ru service is in place; To assign, based on the Client subsystem facilities, to System Users an IP address/list of IP addresses of the Client subsystem PCs with a view to ensure control on the side of the Bank; To provide for availability on a dedicated PC of malware protection facilities, as well as to ensure their operability and regular updating; To preclude opening on dedicated PCs of letters with enclosures received from unknown or untrusted sources; To make use exclusively of licensed software and operating system; To organize regular installation of software and operating system protection updates; To rule out use of remote administration tools; To put in place a licensed network firewall (it is allowed to use personal network firewalls); To carry out a set of organizational arrangements to ensure information security (operating system security settings, restriction of right to access an information system, pass-wording, preparation of incident response procedures, etc.); To monitor security requirements compliance.

операционной системы, ограничение прав доступа информационной системы, организация парольной защиты, подготовка процедур реагирования на инциденты и т.п.); Контролировать соблюдение требований безопасности.	
3.2.2. Для работы с Мобильным устройством: Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы; Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы; Исключить использование средств удаленного администрирования; Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты); Контролировать соблюдение требований безопасности; Обеспечить наличие антивирусного программного обеспечения.	3.2.2. With regard to a mobile device operation: To make use exclusively of licensed software and operating systems; To arrange regular software and operating system updating; To preclude use of remote administration tools; To perform a set of organizational measures to ensure information security (operating system security settings, restriction of right to access an information system, pass-wording); To monitor security requirements compliance; To roll out anti-virus software.
3.3. Пользователи Системы, уполномоченные использовать Систему Клиентами, относящимися к сегменту предпринимателей, должны в Системе ввести номер телефона сотовой связи для получения на указанный номер информационных сообщений в соответствии с Договором.	3.3. System Users authorized by business segment Clients to use the System are obliged to enter into the System a mobile phone number in order to receive to such phone number information messages in accordance with the Agreement.
3.4. Клиент обязан: Исключить появление на Персональном компьютере или Мобильном устройстве подсистемы «Клиент» вирусов и других программ деструктивного действия, которые могут разрушить или модифицировать программное обеспечение подсистемы, скомпрометировать ключи Пользователя Системы посредством применения лицензионных средств защиты от вредоносного кода и регулярного их обновления;	3.4 The Client is obliged: To eliminate penetration of viruses and other destructive software into PCs or mobile devices of the Client subsystem which may destroy or modify the subsystem software, compromise the System Users' keys, which protection should rely on application of licensed malware protection facilities and regular updating thereof; To rule out a possibility to introduce unauthorized modifications in the Clients' hardware

Исключить возможность несанкционированных Банком изменений в технических и программных средствах Клиента, определенных в Списке; Исключить возможность Компрометации ключей в процессе их транспортировки, эксплуатации и хранения.	and software specified in the List not authorized by the Bank; To preclude a possibility of compromise of keys in the course of their transportation, operation and safe-keeping.
3.5. Стороны обязаны: обеспечивать конфиденциальность Ключей электронных подписей, в частности не допускать использование принадлежащих им Ключей электронных подписей без их согласия; уведомлять другую Сторону о нарушении конфиденциальности Ключа электронной подписи (Компрометации ключа) в течение не более чем одного рабочего дня со дня получения информации о таком нарушении; не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.	3.5. The Parties are obliged: To ensure confidentiality of ES keys. In particular, it is not allowed to use the Parties' ES keys without their consent; To notify the other Party about violation of confidentiality of an ES key (Key Compromise) within not more than one business day following the receipt of information concerning such violation; Not to use ES key, if there are reasons to believe that confidentiality of a key was breached.
3.6. Банк вправе в одностороннем порядке заблокировать Ключ электронной подписи Пользователя Системы в случае появления обоснованных подозрений в наличии на Персональном компьютере и/или Мобильном устройстве Пользователя Системы вирусов или других программ деструктивного действия. Блокировка Ключа электронной подписи. Пользователя Системы снимается Банком по факту получения от Клиента подтверждения об удалении с Персонального компьютера и/или Мобильного устройства Пользователя Системы вирусов или других программ деструктивного действия.	3.6. The Bank has the right to unilaterally lock a System User's ES key in case there is reasonable suspicion of virus infection or penetration of other malware in a PC and/or mobile device. ES key locking is realized by the Bank following receipt by the Client of confirmation on removal of viruses and other malware from a PC and/or a System User's mobile device.
3.7. В случае возникновения угрозы Компрометации ключей регламентируется следующая последовательность действий Сторон. Если произошла Компрометация ключей любого Пользователя Клиента, последний обязан: В случае доступности Комплекта ключей (подозрение на несанкционированное копирование) немедленно послать в Банк ЭД «Блокировка ключа». При этом Система автоматически заблокирует возможность	3.7. In case there is a threat of a Key Compromise, the following response sequence of the Parties is established. In case of a compromise of keys of any User of the Client, the latter is obliged: If a set of keys is available (suspicion of unauthorized copying), to immediately send to the Bank a Key Locking electronic message, following which the System will automatically block a

использования данного Комплекта ключей Пользователя Системы; В случае недоступности (утрата, хищение и т.п.) Комплекта ключей сообщить Администратору Системы по телефону (телефон и электронный адрес Администратора системы указаны на сайте www.bankline.ru, а также в Заявлении, используя для авторизации кодовую фразу, приведенную в Сертификате ключа, о факте Компрометации ключей; В случае утраты Пользователем Системы кодовой фразы Администратор Системы вправе произвести дополнительные действия по авторизации Пользователя Системы (обратный звонок по указанному в Заявлении телефону, запрос на предоставление дополнительной информации: о фамилии куратора Клиента в Банке/уполномоченного сотрудника Банка, количестве пользователей и т.п.). В случае предоставления необъективной информации Администратор ставит в известность куратора Клиента в Банке/уполномоченного сотрудника Банка и по согласованию с ним решает вопрос о продолжении/блокировании работы Клиента в Системе; В случае компрометации (утраты, разглашения) SMS-кода незамедлительно проинформировать Банк по любому каналу связи; В срок не более трех рабочих дней после сообщения по телефону о факте Компрометации ключей направить в Банк на бланке Клиента письменное объяснение случившегося, заверенное надлежащим образом подписями уполномоченных лиц и печатью Клиента (при наличии). В письме должно содержаться распоряжение Банку о приостановлении дальнейшей обработки ЭД до устранения причин случившегося и (или) замены Комплекта ключей; В случае принятия решения о замене Комплекта ключей, сгенерированного для Персонального компьютера, сгенерировать новый Комплект ключей самостоятельно и направить своего представителя в Банк для его регистрации. В случае принятия решения о замене Комплекта ключей, сгенерированного посредством Мобильного приложения, сгенерировать новый Комплект ключей самостоятельно в соответствии с Порядком.	possibility for System Users to use the compromised set of keys; If a set of keys is not available (as a result of loss, theft, etc.), to notify the System Administrator via phone (the System Administrator's phone number and electronic address are available on the web-site at www.bankline.ru, as well as in the Application, by using a code phrase for authorization specified in the Key Certificate with a view to report a Key Compromise; In case of loss by a System User of a code phrase, the System Administrator is entitled to undertake additional actions on a System User's authorization (dial back the phone number specified in the Application, send a request for additional information, i.e. full name of the Client's curator on the side of the Bank/authorized Bank officer, number of users, etc.). In case unreliable information is furnished, the System Administrator is to notify the Client's curator on the side of the Bank/authorized Bank officer, and to take a decision based on the latter's consent, to continue/block the Client's work in the System; In case of a compromise (loss, disclosure) of SMS-code, it is necessary to immediately notify the Bank via any communication channel; Within not more than three business days following the phone call on a key compromise, to submit to the Bank a written account of the incident executed on the Client's letterhead duly certified by the signatures of authorized persons and the Client's seal attached (if available). The said written statement is to carry an instruction to the Bank to suspend further processing of electronic documents pending elimination of the reasons underlying the incident and/or to replace the keys; In the event a decision is taken to replace the set of keys generated for a PC, to independently regenerate a new set of keys and send its representative to the Bank with a view to register such new set of keys. In the event a decision is taken to replace the set of keys generated with use of a mobile application, to independently regenerate a new set of keys in accordance with the Procedure. In case of a compromise of a set of keys of the Bank, the latter is obliged: To notify the Client about the compromise of the Bank's set of keys, continuation/suspension of

Если произошла Компрометация ключей Банка, последний обязан: Известить Клиента о факте компрометации Комплекта ключей Банка, продолжении\приостановлении работы Системы и смене Комплекта ключей Банка посредством Системы с указанием даты и точного времени смены вышеуказанного Комплекта ключей; Произвести внеплановую смену Комплекта ключей Банка, опубликовать новый Ключ проверки электронной подписи и копию Сертификата ключа Банка, содержащего новый Ключ проверки электронной подписи Банка, на сервере Системы.	operation of the System and replacement of the set of keys of the Bank by using the System facilities with indication of the date and exact time of such replacement; To carry out an unscheduled replacement of the Bank's set of keys, to publish a new ES verification key and a copy of the Bank's Key Certificate with a new ES verification key of the Bank on the System server.
3.8. При получении по телефону сообщения о возникновении угрозы Компрометации ключей от авторизованного по кодовой фразе Клиента Банк немедленно приостанавливает использование Системы данным Клиентом. С этого момента операции проводятся только на основании документов, оформленных в бумажном виде. Дальнейшее использование Системы Клиентом возможно только после устранения угрозы Компрометации ключей Клиента.	3.8. When notified by the Client authorized with use of a code phrase via the phone about a threat of a compromise of keys, the Bank will immediately suspend such Client's work in the System. Thereafter operations may only be performed on the basis of paper documents. Further use of the System by the Client is only possible following elimination of a threat of compromise of the Client's keys.

II. При использовании Подсистемы «Прямая интеграция» / With regard to use *Direct integration* subsystem

4. Общие правила обмена электронными документами / General rules of exchange of electronic documents

4.1. Клиент самостоятельно определяет способ интеграции учетной системы и Банка. Банк поддерживает следующие варианты интеграции (каждому из вариант интеграции соответствует свой набор электронных документов): • через сервис «1С:ДиректБанк»; • через протокол SOAP/FTPs; • через сервис «Транзит НРД» (транзит документов Клиентов через систему электронного документооборота Небанковской кредитной организации акционерного общества «Национальный расчетный депозитарий» (ИНН 7702165310));	4.1. The Client independently determines the method of integration of the accounting system and the Bank. The Bank supports the following integration options (each of the integration options has its own set of electronic documents): • via the *1S: DirectBank* service; • via the *SOAP* / *FTPs* Protocol; • via the *TransitNSD* service (transit of Clients' documents through the electronic document management system of the National Settlement Depository Joint Stock Company (TIN 7702165310); • via the *CyberFT* network (transit of Clients' documents through the electronic document

• через сеть «CyberFT» (транзит документов Клиентов через систему электронного документооборота Общества с ограниченной ответственностью «КИБЕРПЛАТ» (ИНН 7731220815).	management system of the CYBERPLAT Limited Liability Company (TIN 7731220815)).
4.2. Для работы в Подсистеме «Прямая интеграция» Клиент самостоятельно производит настройки учетной системы и выполняет необходимые доработки своей системы в зависимости от выбранного способа интеграции с Банком.	4.2. To work in the «Direct Integration» Subsystem, the Client independently makes settings for the accounting system and makes the necessary modifications to his system, depending on the chosen method of integration with the Bank.
4.3. Для подключения к Банку по выбранному каналу прямого обмена Клиент использует: • web-сервис «1С:ДиректБанк», опубликованный Банком по адресу https://www.bankline.ru/h2h/db1c; • SOAP-сервер, опубликованный Банком по адресу https://www.bankline.ru/h2h/iso/H2HService; • FTPs-ресурс, предоставленный Банком персонально каждому клиенту; • интеграционный сервис «Транзит 2.0», предоставляемый НКО АО НРД; • интеграционный сервис «CyberFT», предоставляемый ООО «КИБЕРПЛАТ».	4.3. To connect to the Bank via the selected direct exchange channel, the Client uses: • *1S: DirectBank* web service published by the Bank at https://www.bankline.ru/h2h/db1c; • *SOAP* server published by the Bank at https://www.bankline.ru/h2h/iso/H2HService; • *FTPs*-resource provided by the Bank personally to each client; • Integration service *Transit 2.0* provided by NCO JSC NSD; • *CyberFT* integration service provided by CYBERPLAT LLC.
4.4. Банк поддерживает следующие типы электронных документов в зависимости от выбранного варианта интеграции: • «1С:ДиректБанк»: o документы от Клиента: - платежные поручения в рублях РФ; - платежные поручения в валюте; - зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке; o документы от Банка: - статус исполнения платежного поручения; - подтверждение зачисления денежных средств на счета сотрудников; - выписки по рублевым и валютным счетам. • протокол «SOAP» / «FTPS»: o документы от Клиента:	4.4. The bank supports the following types of electronic documents, depending on the chosen integration option: • *1S: DirectBank*: o documents from the Client: - payment orders in rubles of the Russian Federation; - payment orders in foreign currency; - payroll registers for the distribution of salaries to employees to accounts in the Bank; o documents from the Bank: - the status of execution of the payment order; - confirmation of crediting funds to employees' accounts; - statements of ruble and foreign currency accounts. • *SOAP / FTPS* protocol: o documents from the Client:

- платежные поручения в рублях РФ и валюте; - заявления на покупку/продажу валюты; - заявления об обязательной продаже валюты; - зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке; - документы валютного контроля; - заявления о размещении денежных средств; - документы свободного формата; - запросы на отзыв документа. o документы от Банка: - статус исполнения платежного поручения; - подтверждение зачисления денежных средств на счета сотрудников; - выписки; - статус отзыва документа. • через «Транзит НРД»/сеть «CyberFT»: o документы от Клиента: - платежные поручения в рублях РФ и валюте; - заявления на покупку/продажу валюты; - заявления об обязательной продаже валюты; - зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке; - документы валютного контроля; - заявления о размещении денежных средств; - документы свободного формата; o документы от Банка: - статус исполнения платежного поручения; - подтверждение зачисления денежных средств на счета сотрудников; - выписки.	- payment orders in rubles of the Russian Federation and foreign currency; - foreign currency purchase/sale orders; - foreign currency surrender applications; - payroll registers for the distribution of salaries to employees to accounts in the Bank; - foreign exchange control documents; - applications for the placement of funds; - free format documents; - requests for document revocation. o documents from the Bank: - the status of execution of the payment order; - confirmation of crediting funds to employees' accounts; - extracts; - document revocation status. • through *TransitNSD / CyberFT* network: o documents from the Client: - payment orders in rubles of the Russian Federation and foreign currency; - foreign currency purchase/sale orders; - foreign currency surrender applications; - payroll registers for the distribution of salaries to employees to accounts in the Bank; - documents of currency control; - applications for the placement of funds; - free format documents; o documents from the Bank: - the status of execution of the payment order; - confirmation of crediting funds to employees' accounts; - extracts.

4.5. Банк поддерживает следующие форматы электронных документов в зависимости от выбранного варианта интеграции: • «1С:ДиректБанк»: XML-формат технологи DirectBank (ДиректБанк) фирмы 1С. Описание приведено на сайте компании по адресу https://v8.1c.ru/its/services/1c-direktbank/. • «SOAP» / «FTPS»: XML-формат стандарта ISO 20022: o для платежей в рублях РФ на базе формата pain.001.001.03 (06) o для статусов исполнения платежей на базе формата pain.002.001.03 (06) o для выписок по окончанию операционного дня на базе формата camt.053.001.02 o для промежуточных выписок по запросу на базе формата camt.052.001.02 o для платежей в валюте и конверсии на базе формата pain.001.001.03 (06) o для отзывов поручений клиента на базе формата camt.055.001.06 o для постановки на учет кредитного договора/контракта на базе формата auth.018.001.01 o для внесения изменений в ВБК на базе формата auth.021.001.01 o для снятия с учета контракта на базе формата auth.020.001.01 o для сведений о валютных операциях на базе формата auth.024.001.01 o для справки о подтверждающих документах на базе формата auth.025.001.01 o для статусов по документам Валютного контроля на базе формата auth.027.001.01 o для возврата ранее размещенных денежных средств на базе формата trea.325.001.01.RU o для подтверждения о размещении депозита на базе формата trea.320.001.01.RU o для писем свободного формата из/в банк auth.026.001.01 Детальное описание форматов предоставляется Банком в Правилах Имплементации (TIG).	4.5. The bank supports the following formats of electronic documents, depending on the chosen integration option: • *1S: DirectBank*: XML-format of DirectBank technology (DirectBank) from 1S. The description is given on the company's website at https://v8.1c.ru/its/services/1c-direktbank/. • *SOAP / FTPS*: ISO 20022 XML format: o for payments in rubles of the Russian Federaion based on the pain.001.001.03 (06) format o for statuses of payment execution based on the pain.002.001.03 (06) format o for statements at the end of the transaction day based on the camt.053.001.02 format o for interim statements upon request based on the camt format. 052.001.02 o for payments in currency and conversion based on the pain.001.001.03 (06) format o to revoke customer orders based on camt.055.001.06 format o for registering a loan agreement / contract based on the auth.018.001.01 format o to make changes to the VBC based on the auth.021.001.01 format o to deregister a contract based on the auth.020.001.01 format o for information about currency transactions based on the auth.024.001.01 format o for information about supporting documents based on auth.025.001.01 format o for statuses for documents of Currency control based on auth.027.001.01 format o to return previously placed funds based on the trea.325.001.01.RU format o to confirm the placement of a deposit based on the trea.320.001.01.RU format o for free format letters from / to the bank auth.026.001.01 A detailed description of the formats is provided by the Bank in the Rules of Implementation (TIG). • *TransitNSD / CyberFT* network: ISO 20022 XML format: o for payments based on the pain.001.001.03 (06) format

• «Транзит НРД»/сеть «CyberFT»: XML-формат стандарта ISO 20022: о для платежей на базе формата pain.001.001.03 (06) о для статусов исполнения платежей на базе формата pain.002.001.03 (06) о для выписок по окончанию операционного дня на базе формата camp.053.001.02.	o for statuses of payment execution based on the pain.002.001.03 (06) format o for statements at the end of the business day based on the camp.053.001.02 format.
4.6. Для начала работы в Системе Пользователь Системы должен быть зарегистрирован в Системе, иметь действующий Сертификат и соответствующий ему Закрытый ключ.	4.6. To start working in the System, the System User must be registered in the System, have a valid Certificate and the corresponding Private Key.
4.7. Работа с ЭД в Системе происходит с ЭД, подписанными ЭП Клиента с помощью действующего Сертификата. Банк исполняет ЭД, полученные от Клиента, только после успешной проверки ЭП Клиента сервером Системы. ЭП Клиента под пакетом документов приравнивается к ЭП Клиента под каждым документом внутри пакета.	4.7. The work with ED in the System is carried out with ED signed by the Client's ES using a valid Certificate. The Bank executes ED received from the Client only after successful verification of the Client's ES by the System server. The Client's ES under the package of documents is equal to the Client's ES under each document within the package.
4.8. Клиент может создать неограниченное количество Сертификатов для работы в Системе. При этом количество единовременно используемых Сертификатов для подписания ЭД ЭП Клиента: • для технологии «1С:ДиректБанк» - не более 4 (четырех) Сертификатов; • для технологий на базе протокола «SOAP» / «FTPS» / «Транзит НРД» /сети «CyberFT» – не ограничено.	4.8. The Client can create an unlimited number of Certificates to work in the System. At the same time, the number of Certificates used at a time for signing the Client's EDS: • for *1S: DirectBank* technology - no more than 4 (four) Certificates; • for technologies based on the *SOAP* / *FTPS* / *TransitNSD* / *CyberFT* network - unlimited.
4.9. Для технологии на базе протокола «SOAP» / «FTPS» /«Транзит НРД» / сети «CyberFT» Клиент может установить дополнительные требования к подписанию ЭД по сумме, заполнив соответствующий раздел Заявления о настройке пользователей системы и перечне электронных документов подсистемы «Прямая интеграция» при наличии открытого расчетного счета (Приложение 1.2 к Условиям). В этом случае ЭД, получаемый Банком, должен быть сформирован таким образом, чтобы удовлетворять требованиям сочетания ЭП Клиента как для верификации на сервере Подсистемы «Прямая интеграция», так и для дополнительной проверки подписей на базе Заявления о дополнительной настройке подписей по типам электронных	4.9. For technology based on the *SOAP / FTPS / TransitNSD / CyberFT* network, the Client can set additional requirements for signing ED by amount by filling out the appropriate section of the Statement on setup of users of the system and the list of electronic documents of the subsystem of *Direct Integration* in the presence of an open current account (Annex 1.2 to the Terms). In this case, the ED received by the Bank must be formed in such a way as to meet the requirements of the Client's ES combination both for verification on the server of the *Direct Integration* Subsystem, and for additional verification of signatures based on the Application for additional configuration of signatures by types of electronic documents. In the event that the Client already has a valid agreement to work in *ICB*

документов. В случае, если Клиент уже имеет действующее соглашение для работы в подсистеме «ИКБ» и требования к подписанию ЭД, настроенные в подсистеме «ИКБ», то данные требования будут применяться к ЭД, полученным по Подсистеме «Прямая интеграция» до отмены такого требования.	Subsystem and the requirements for signing ED, configured in the *ICB* subsystem, then these requirements will apply to ED received through the Subsystem *Direct integration* until such a requirement is canceled.
4.10. Процедура обработки ЭД сервером Подсистемы «Прямая интеграция» происходит следующим образом: • сервер Банка получает ЭД и проверяет корректность всех имеющихся в нем ЭП. • основанием для принятия Банком ЭД, переданного Клиентом по Подсистеме «Прямая интеграция», является наличие в количестве, установленном в соответствии с Заявлением, и корректность всех ЭП Клиента под ЭД. При положительном результате проверки сервер Банка проставляет в ЭД отметку о времени и ЭП Банка, свидетельствующую о получении пакета Банком, и сохраняет данный документ в Подсистеме «Прямая интеграция». При отрицательном результате проверки ЭП Клиента ЭП Банка в документе не проставляется, Клиент получает сообщение об ошибке средствами Подсистемы «Прямая интеграция». Сертификат ключа ЭП Банка выпускается уполномоченным представителем Банка. Срок действия Комплекта ключей Банка составляет 1 (один) год.	4.10. The procedure for processing ED by the server of the *Direct Integration* Subsystem is as follows: • the Bank's server receives the ED and checks the correctness of all the ES in it. • the basis for the Bank's acceptance of the ED transmitted by the Client via the *Direct Integration* Subsystem is the availability in the quantity set in accordance with the Statement and the correctness of all the Client's ES under the ED. If the check is positive, the Bank's server puts a time stamp and the Bank's electronic signature in the ED, indicating that the Bank has received the package, and saves this document in the *Direct Integration* Subsystem. In case of a negative result of verification of the Client's ES, the Bank's ES is not entered in the document, the Client receives an error message using the *Direct Integration* Subsystem. An authorized representative of the Bank issues the ES Bank key certificate. The Bank's Key Set is valid for 1 (one) year.
4.11. Документ считается переданным Клиентом в Банк, если он сохранен в архиве исходящих документов Клиента на сервере Банка. При наличии действующего договора для работы в подсистеме «ИКБ» все входящие документы будут отображаться в «Исходящих документах» Клиента на сервере Банка. Клиент может сохранить любой исходящий документ в файл для ведения собственного архива. Файл содержит ЭП Клиента, отметку о времени приема документа Банком и ЭП Банка. Файлы с сервера Банка и из архива Клиента могут затем использоваться при процедуре разрешения разногласий между Сторонами.	4.11. A document is considered to be transferred by the Client to the Bank if it is stored in the archive of the Client's outgoing documents on the Bank's server. If there is a valid agreement for work in the *ICB* subsystem, all incoming documents will be displayed in the "Outgoing documents" of the Client on the Bank's server. The client can save any outgoing document to a file to maintain its own archive. The file contains the Client's electronic signature, the time stamp of the document acceptance by the Bank and the Bank's electronic signature. Files from the Bank's server and from the Client's archive can then be used in the procedure for resolving disagreements between the Parties.
4.12. Переданный Клиентом в Банк документ в каждый момент времени имеет на сервере Банка определенный статус с отметкой времени его получения. Статус документа изменяется Банком. Клиент имеет возможность	4.12. The document sent by the Client to the Bank at each moment of time has a certain status on the Bank's server with a time stamp of its receipt. The status of the document is changed by the Bank. The Client has the opportunity to constantly receive

постоянно получать на сервере Банка информацию об изменении статуса (в том числе о времени его изменения) переданного в Банк документа. Сервер Банка присваивает полученным от Клиента документам следующие статусы: • для технологии «1С:ДиректБанк»: o Платежные поручения в рублях РФ, платежные поручения в валюте: - «Принят» – электронный документ прошел первичный контроль и поступил в обработку; - «Исполнен» – платежный документ исполнен Банком; - «Отклонен банком» – электронный документ не прошел первичный контроль в Банке и был отклонен; - «Приостановлен» – платежный документ отложен Банком по причине недостатка средств на счете Клиента; - «Аннулирован» – Электронный документ был отозван Клиентом с одобрения Банка; - «Не подтвержден» – Платежный документ ожидает подтверждения по SMS или личном кабинете Клиента; o Зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке: - «Принят» – электронный документ прошел первичный контроль и поступил в обработку; - «Исполнен» – электронный документ исполнен Банком; - «Отклонен банком» – электронный документ не прошел первичный контроль в Банке и был отклонен;. Стороны признают, что надлежащим уведомлением Банком Клиента о приеме к исполнению ЭД Клиента будет являться присвоение Банком ЭД Клиента статуса «Принят». Банк информирует Клиента об исполнении каждого ЭД Клиента путем направления Клиенту соответствующего уведомления посредством Подсистемы «Прямая интеграция». • для технологии SOAP/FTPS/«Транзит НРД»/сети «CyberFT» используются следующие статусы: «RCVD» - получено Банком;	information on the status change (including the time of its change) of the document sent to the Bank on the Bank's server. The Bank's server assigns the following statuses to the documents received from the Client: • for technology *1S: DirectBank*: o Payment orders in rubles of the Russian Federation, payment orders in foreign currency: - “Accepted” - the electronic document has passed the initial control and has been processed; - “Executed” - the payment document was executed by the Bank; - “Rejected by the bank” - the electronic document did not pass the initial control in the Bank and was rejected; - "Suspended" - the payment document has been postponed by the Bank due to insufficient funds on the Client's account; - “Canceled” - the electronic document was revoked by the Client with the approval of the Bank; - "Not confirmed" - The payment document is awaiting confirmation by SMS or the Client's personal account; o Payroll registers for the distribution of salaries to employees to accounts with the Bank: - “Accepted” - the electronic document has passed the initial control and has been processed; - "Executed" - the electronic document was executed by the Bank; - “Rejected by the bank” - the electronic document did not pass the initial control in the Bank and was rejected; The Parties acknowledge that a proper notification by the Bank of the Client about the acceptance of the Client's ED for execution will be the Bank's assignment of the “Accepted” status to the Client's ED. The Bank informs the Client about the execution of each of the Client's ED by sending the corresponding notification to the Client via the Direct Integration Subsystem. • for *SOAP / FTPS / Transit NSD / CyberFT* network, the following statuses are used: “RCVD” - received by the Bank; "RJCT" - rejected; "ACTC" - Accepted, Authenticity and Format Verified;

«RJCT» - отклонено; «ACTC» - принято, проверены подлинность и формат; «ACCP» - принято, документ отправлен на исполнение; «ACSP» - конечный успешный для внешних платежей; «ACSC» - конечный успешный для внутренних платежей.	"ACCP" - accepted, the document has been sent for execution; "ACSP" - final successful for external payments; "ACSC" - Ultimate Successful for Domestic Payments.
4.13. При формировании ЭД для Клиента Банк проставляет в нем ЭП Банка. Документ считается переданным Банком Клиенту, если он подписан ЭП Банка и помещен во входящие документы Клиента на сервере Банка. При наличии действующего договора для работы в Подсистеме «ИКБ», исходящие документы от Банка будут присутствовать в списке «Входящие документы» Клиента на сервере Банка. Клиент может сохранить любой входящий документ в файл для ведения собственного архива. Файлы архива могут затем использоваться при разрешении разногласий.	4.13. When generating the ED for the Client, the Bank puts down the Bank's ES in it. A document is considered transferred by the Bank to the Client if it is signed by the Bank's electronic signature and placed in the Client's incoming documents on the Bank's server. If there is a valid agreement for work in the *ICB* Subsystem, outgoing documents from the Bank will be present in the list of "Incoming documents" of the Client on the Bank's server. The client can save any incoming document to a file to maintain its own archive. The archive files can then be used to resolve the dispute.
4.14. Банк фиксирует электронные архивы полученных от Клиента ЭД, содержащих ЭП Клиента и ЭП Банка, и доставленных Клиенту ЭД, содержащих ЭП Банка, и хранит их.	4.14. The Bank records the electronic archives of the ED received from the Client, containing the Client’s ES and the Bank’s ES, and the EDs delivered to the Client, containing the Bank’s ES, and stores them.

5. Порядок получения, замены и хранения ключей / Procedure for obtaining, replacing and storing keys

5.1. Клиент может запросить генерацию Сертификатов своих Пользователей Подсистемы «Прямая интеграция» согласно Заявлению о настройке пользователей системы (Приложение 1.2, Приложение 1.3 к Условиям) в соответствии с Руководством по генерации сертификатов электронной подписи пользователя для Подсистемы «Прямая интеграция», опубликованном на сайте Банка. В рамках Договора Клиент может использовать сертификаты ЭП, выпущенные Банком для Пользователей Клиента в рамках заключенного договора об использовании электронных документов.	5.1. The Client can request the generation of Certificates of its Users of the *Direct Integration* Subsystem in accordance with the Statement on setup of users of the system (Annex 1.2, Annex 1.3 to the Terms) in accordance with the Guidelines for Generating User Electronic Signature Certificates for the *Direct Integration* Subsystem, published on the Bank's website. Within the framework of the Agreement, the Client can use the ES certificates issued by the Bank for the Client's Users within the framework of the concluded Agreement on the use of electronic documents.

5.2. Сертификат каждого Пользователя Подсистемы «Прямая интеграция» регистрируется Банком на основании подписанного Сторонами Акта о признании открытого ключа Подсистемы «Прямая интеграция» (размещен на веб-сайте https://www.bankline.ru), распечатанного и подписанного в 2 (двух) экземплярах, по одному для каждой из Сторон. Заполненный Акт Система формирует автоматически.	5.2. The certificate of each User of the *Direct Integration* Subsystem is registered by the Bank on the basis of the Act on recognition of the public key of the *Direct Integration* Subsystem signed by the Parties (posted on the website https://www.bankline.ru), printed and signed in 2 (two) copies , one for each of the Parties. The completed Act is automatically generated by the System.
5.3. Срок действия Комплекта ключей указывается в Сертификате и составляет 1 (Один) год. Срок действия Сертификата не может превышать срок действия полномочий Пользователя Системы в соответствии с документами, подтверждающими его полномочия. В случае если исходя из представленных Клиентом документов не представляется возможным установить срок действия полномочий Пользователя Подсистемы «Прямая интеграция», срок действия Комплекта ключей не может превышать 1 (Одного) года. Клиент несет ответственность за отслеживание срока действия сертификата и полномочий Пользователей Клиента.	5.3. The validity period of the Key Set is indicated in the Certificate and is 1 (One) year. The validity period of the Certificate cannot exceed the validity period of the System User's powers in accordance with the documents confirming his powers. If, based on the documents submitted by the Client, it is not possible to establish the term of the User's powers of the *Direct Integration* Subsystem, the term of the Key Set may not exceed 1 (One) year. The Client is responsible for keeping track of the certificate validity period and the authority of the Client's Users.
5.4. До истечения установленного срока Клиент обязан инициировать процедуру генерации нового Сертификата. Продление срока действия Сертификата невозможно. На основании Заявления об отзыве (аннулировании) сертификата, составленном в свободном формате, Сертификат Пользователя Подсистемы «Прямая интеграция» аннулируется и не подлежит восстановлению. Каждый новый Акт о признании конкретного Пользователя, подписанный Сторонами, автоматически отменяет действие Сертификата данного Пользователя Подсистемы «Прямая интеграция», выпущенного ранее.	5.4. Before the expiration of the established period, the Client is obliged to initiate the procedure for generating a new Certificate. Renewal of the Certificate is not possible. On the basis of the Statement for revocation (cancellation) of the certificate, drawn up in a free format, the User Certificate of the *Direct Integration* Subsystem is canceled and cannot be restored. Each new Certificate of Recognition of a specific User, signed by the Parties, automatically cancels the validity of the Certificate of this User of the *Direct Integration* Subsystem issued earlier.
5.5. Оформленный со стороны Банка Акт о признании Клиента вручается лично представителю Клиента, курьеру Клиента, либо направляется Клиенту посредством почтовой связи. Акт о признании должен храниться у каждой из Сторон не менее 5 (Пяти) лет после окончания срока действия Комплекта ключей.	5.5. The Client Recognition Act drawn up by the Bank is handed over personally to the Client's representative, the Client's courier, or sent to the Client by mail. The act of recognition must be kept by each of the Parties for at least 5 (Five) years after the expiration of the Key Set.
5.6. Обязательное аннулирование Сертификата проводится в случае Компрометации Ключей электронной подписи Клиента.	5.6. Mandatory revocation of the Certificate is carried out in case of Compromise of the Client's electronic signature Keys.

5.7. В случае лишения Клиентом Пользователя Подсистемы «Прямая интеграция» права подписывать ЭП Клиента ЭД, соответствующий Сертификат выводится из действия на основании письменного Заявления об отзыве (аннулировании) сертификатов пользователей Подсистемы «Прямая интеграция», составленного в свободном формате.	5.7. If the Client deprives the User of the *Direct Integration* Subsystem of the right to sign the Client's electronic signature of the ED, the corresponding Certificate is withdrawn from action on the basis of a written Statement for revocation (cancellation) of certificates of users of the *Direct Integration* Subsystem, drawn up in a free format.

6. Обеспечение безопасности процедуры обмена документами / Ensuring the security of the document exchange procedure

6.1. Безопасность обмена ЭД достигается за счет применения следующих средств:	6.1. The security of ED exchange is achieved through the use of the following means:
6.1.1. Использованием СКЗИ «Криптотокен 2 ЭП» в составе USB-токенов JaCarta-2 ГОСТ, разработанных АО «Аладдин Р.Д.» (сертификат соответствия № СФ/124-3956 от 17 ноября 2020 года). Ключ электронной подписи никогда не покидает внутренней защищенной памяти USB-токена. Генерация и хранение Ключа электронной подписи, а также подписание документов производится во внутренней защищенной памяти USB-токена. Доступ к ключу электронной подписи осуществляется с использованием ПИН-кода доступа к токену;	6.1.1. Utilization of CIPF Cryptotoken 2 ES in conjunction with USB tokens JaCarta-2 GOST developed by JSC Aladdin R.D. (certificate of conformity issued by the Federal Security Service (FSB) of the Russian Federation (FSB) No. SF/124 – 3956 of November 17, 2020). An electronic signature key is never detached from the internal protected memory of a USB token. ES keys are generated and signing of documents is performed inside the internal protected memory of a USB token. Access to ES key is obtained with use of the PIN access code to the token.
6.1.2. СКЗИ КриптоПро CSP версии 4.x и выше. Для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол Transport Layer Security (TLS v. 1.2, RFC 2246), применяются криптографические алгоритмы шифрования в соответствии с ГОСТ 34.13-2018, ГОСТ 34.12-2018, хэширования в соответствии с ГОСТ Р 34.11-2012;	6.1.2. CIPF CryptoPro CSP of version 4.0 and higher. With a view to protect data from unauthorized access in telecommunication channels, protocol Transport Layer Security (TLS v. 1.2, RFC 2246) is used, cryptographic encryption algorithms are used in accordance with GOST 34.13-2018, GOST 34.12-2018, hashing in accordance with GOST R 34.11-2012.
6.1.3. Удостоверения принадлежности сервера Подсистемы ПАО РОСБАНК с помощью сертификата, выданного ПАО РОСБАНК аккредитованным Удостоверяющим центром ООО «КРИПТО-ПРО».	6.1.3. Certificates of ownership of the server of the Subsystem of PJSC ROSBANK using a certificate issued by PJSC ROSBANK by an accredited Certification Center LLC CRYPTO-PRO.
6.2. На основании дополнительных соглашений между Сторонами возможно применение других технических средств по защите информации.	6.2. On the basis of additional agreements between the Parties, it is possible to use other technical means to protect information.
6.3. Клиенту рекомендуется обеспечить комплекс организационно-технических мер,	6.3. The client is recommended to provide a set of organizational and technical measures aimed at meeting the following safety requirements:

направленных на выполнение следующих требований безопасности:	
6.3.1. Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;	6.3.1. To ensure the use of exclusively licensed software and operating system;
6.3.2. Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;	6.3.2. To organize regular installation of software and operating system security updates;
6.3.3. Исключить использование средств удаленного администрирования;	6.3.3. To exclude the use of remote administration tools;
6.3.4. Обеспечить применение лицензионного межсетевого экрана (допускается использование персонального межсетевого экрана);	6.3.4. To ensure the use of a licensed firewall (it is allowed to use a personal firewall);
6.3.5. Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты, подготовка процедур реагирования на инциденты и т.п.);	6.3.5. To carry out a set of organizational measures to ensure information security (setting up the security of the operating system, restricting access rights to the information system, organizing password protection, preparing procedures for responding to incidents, etc.);
6.3.6. Контролировать соблюдение требований безопасности.	6.3.6. To monitor compliance with safety requirements.
6.4. Клиент обязан:	6.4. The clients is obliged:
6.4.1. исключить появление в компьютере вирусов и других программ деструктивного действия, которые могут разрушить или модифицировать программное обеспечение Подсистемы «Прямая интеграция», скомпрометировать ключи Пользователя Подсистемы посредством применения лицензионных средств защиты от вредоносного кода и регулярного их обновления;	6.4.1. to exclude the appearance in the computer of viruses and other destructive programs that can destroy or modify the software of the *Direct Integration* Subsystem, compromise the Subsystem User's keys by using licensed means of protection against malicious code and their regular updating;
6.4.2. исключить возможность Компрометации ключей в процессе их эксплуатации и хранения.	6.4.2. to exclude the possibility of compromising keys during their operation and storage;
6.5. Стороны обязаны:	6.5. The Parties are obliged:
6.5.1. обеспечивать конфиденциальность Ключей электронной подписи, в частности не допускать использование принадлежащих им Ключей электронной подписи без их согласия;	6.5.1. to ensure the confidentiality of the Electronic Signature Keys, in particular, prevent the use of the Electronic Signature Keys belonging to them without their consent;
6.5.2. уведомлять другую Сторону о нарушении конфиденциальности Ключа электронной подписи (Компрометации ключа) в	6.5.2. to notify the other Party about the violation of the confidentiality of the Electronic Signature Key (Key Compromise) within no more than

течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении;	1 (One) business day from the date of receipt of information about such violation;
6.5.3. не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного Ключа нарушена.	6.5.3. not to use the Electronic Signature Key if there are reasons to believe that the confidentiality of this Key has been violated.
6.6. Банк вправе в одностороннем порядке заблокировать Ключ электронной подписи Пользователя Подсистемы «Прямая интеграция» в случае появления обоснованных подозрений в наличии на компьютере Пользователя Подсистемы «Прямая интеграция» вирусов или других программ деструктивного действия. Для возобновления работы Клиенту после удаления с компьютера Пользователя Подсистемы «Прямая интеграция» вирусов или других программ деструктивного действия потребуется заново сгенерировать Сертификат и Ключ электронной подписи.	6.6. The Bank has the right to unilaterally block the Electronic Signature Key of the User of the *Direct Integration* Subsystem in the event of reasonable suspicions of the presence of viruses or other programs of destructive action on the User's computer of the *Direct Integration* Subsystem. To resume the work of the Client after removing viruses or other destructive programs from the User's computer of the *Direct Integration* Subsystem, it will be necessary to re-generate the Certificate and the Electronic Signature Key.
6.7. В случае возникновения угрозы Компрометации ключей регламентируется следующая последовательность действий Сторон.	6.7. In the event of a threat of Key Compromise, the following sequence of actions by the Parties is regulated.
6.8. В случае Компрометации ключей любого Пользователя Клиента, Клиент обязан:	6.8. In case of Compromise of the keys of any User of the Client, the Client is obliged to:
6.8.1. В случаях доступности Комплекта ключей (подозрение на несанкционированное копирование), а также в случае недоступности (утрата, хищение и т.п.) Комплекта ключей сообщить Администратору Подсистемы «Прямая интеграция» по телефону (телефон и электронный адрес Администратора Подсистемы «Прямая интеграция» указаны в Заявлении о настройке пользователей Подсистемы «Прямая интеграция») о факте Компрометации или угрозе Компрометации), используя для авторизации данные из Сертификата.	6.8.1. In cases of availability of the Set of keys (suspicion of unauthorized copying), as well as in case of unavailability (loss, theft, etc.) of the Set of keys, inform the Administrator of the *Direct Integration* Subsystem by phone (telephone and email address of the Administrator of the *Direct Integration* Subsystem are indicated in the Application for Configuring Users of the *Direct Integration* Subsystem) about the fact of Compromise or the threat of Compromise), using the data from the Certificate for authorization.
6.8.2. При этом, Администратор Подсистемы «Прямая интеграция» вправе произвести дополнительные действия по авторизации Пользователя Подсистемы «Прямая интеграция» (обратный звонок по указанному в Заявлении телефону, запрос на предоставление дополнительной информации: о фамилии куратора Клиента в Банке/уполномоченного сотрудника Банка, количестве пользователей и т.п.). В случае непредоставления информации Администратор ставит в известность куратора Клиента в Банке/уполномоченного сотрудника Банка и по согласованию с ним решает вопрос о	6.8.2. At the same time, the Administrator of the *Direct Integration* Subsystem has the right to perform additional actions to authorize the User of the *Direct Integration* Subsystem (call back to the phone number specified in the Statement, request for additional information: about the name of the Customer's curator in the Bank / authorized employee of the Bank, the number of users and etc.). In case of failure to provide information, the Administrator notifies the Client's curator at the Bank / authorized employee of the Bank and, in agreement with him, decides on the continuation / blocking of the Client's work in the *Direct Integration* Subsystem.

продолжении/блокировании работы Клиента в Подсистеме «Прямая интеграция».	
6.8.3. В срок не более 3 (Трех) рабочих дней после сообщения по телефону о факте Компрометации ключей, направить в Банк на бланке Клиента письменное объяснение случившегося, заверенное надлежащим образом подписями уполномоченных лиц и печатью Клиента (при наличии). В письме должно содержаться распоряжение Банку о приостановлении дальнейшей обработки ЭД до устранения причин случившегося и (или) замены ключей;	6.8.3. Within a period of not more than 3 (three) business days after the telephone message about the fact of Key Compromise, send to the Bank on the Client's letterhead a written explanation of the incident, duly certified by the signatures of authorized persons and the Client's seal (if any). The letter must contain an order to the Bank to suspend further processing of ED until the causes of the incident are eliminated and (or) the keys are replaced;
6.8.4. В случае принятия решения о замене Комплекта ключей – Клиент обязан сгенерировать новый Комплект ключей самостоятельно и направить своего представителя в Банк для его регистрации.	6.8.4. If a decision is made to replace the Key Set - the Client is obliged to generate a new Key Set on his own and send his representative to the Bank for its registration.
6.9. В случае Компрометации ключей Банка, последний обязан:	6.9. In case of Compromise of the Bank’s keys, the latter is obliged to:
6.9.1. Известить Клиента о факте компрометации Комплекта ключей Банка, продолжении\приостановлении работы Подсистемы «Прямая интеграция» и смене Комплекта ключей Банка посредством Подсистемы «Прямая интеграция» с указанием даты и точного времени смены вышеуказанного Комплекта ключей;	6.9.1. Notify the Client about the fact of compromise of the Bank's Key Set, continuation / suspension of the *Direct Integration* Subsystem and changing the Bank's Key Set via the *Direct Integration* Subsystem, indicating the date and exact time of the change of the above Key Set;
6.9.2. Произвести внеплановую смену Комплекта ключей Банка и передать Сертификат ключа Банка Клиенту.	6.9.2. Perform an unscheduled change of the Bank's Key Set and transfer the Bank's Key Certificate to the Client.
6.10. При получении по телефону сообщения о возникновении угрозы Компрометации ключей от авторизованного Клиента Банк немедленно приостанавливает использование Подсистемы «Прямая интеграция» данным Клиентом. С этого момента операции проводятся только на основании документов, оформленных в бумажном виде или с использованием иных, не связанных с Подсистемой «Прямая интеграция», средств дистанционного обслуживания.	6.10. Upon receipt by phone of a message about a threat of Key Compromise from an authorized Client, the Bank immediately suspends the use of the *Direct Integration* Subsystem by this Client. From this moment, operations are carried out only on the basis of documents drawn up in paper form or using other means of remote service not related to the *Direct Integration* Subsystem.
6.11. Дальнейшее использование Подсистемы «Прямая интеграция» Клиентом возможно только после устранения угрозы Компрометации ключей Клиента.	6.11. Further use of the *Direct Integration* Subsystem by the Client is possible only after the threat of Compromise of the Client's keys has been eliminated.

III. Порядок проверки ЭД и ЭП при разногласиях/ Procedure for verification of ED and ES in the event of dispute

7.1. Для разрешения споров относительно подлинности ЭД по заявлению заинтересованной Стороны, полагающей, что ее права нарушены, Сторонами в двухнедельный срок с даты подачи заявления создается Согласительная комиссия, в присутствии которой производятся все операции по подготовке и проведению процедуры разрешения спора. В состав Согласительной комиссии включаются представители Банка в количестве двух человек и представители Клиента в количестве двух человек, а в случае необходимости (по соглашению Сторон) – независимые эксперты. Представителями Банка и Клиента могут быть назначены как сотрудники этих организаций, так и иные компетентные лица, полномочия которых подтверждаются соответствующими доверенностями.	7.1. With a view to settle disputes regarding ED authenticity following an application of the Party concerned, which claims a breach of its rights, the Parties shall, within two weeks following such application, set up a Conciliation Commission, in the presence of which arrangements will be made to prepare and conduct the procedure of dispute settlement. The Conciliation Commission is to comprise two representatives of the Bank and two representatives of the Client, and if necessary (subject to the Parties' consent) independent experts may be invited to sit on the Commission. Representatives of the Bank and the Client may be appointed from the number of the personnel of such entities, as well as other competent persons whose authority is to be certified by relevant powers of attorney.
7.2. Спорным ЭД является ЭД, в отношении которого одна Сторона предъявляет претензии по его подлинности другой Стороне.	7.2. An ED is deemed to be disputable with regard to which one Party challenges its authenticity to the other Party.
7.3. Процедура проверки подлинности ЭД проводится на оборудовании и в помещении Банка.	7.3. The procedure of verification of authenticity of an electronic document is to be conducted with use of the Bank's equipment and premises.
7.4. В присутствии членов Согласительной комиссии Банк обязан на свободном от программного обеспечения компьютере установить операционную систему Windows7 и выше и программу криптографической проверки ЭП: • Для Подсистемы «ИКБ» - это предоставленная фирмой-разработчиком ЗАО «ИНИСТ» программа проверки ЭП, указанная в п.1.10 настоящего Порядка; • Для Подсистемы «Прямая интеграция» - это программа КриптоПро CSP версии 4.х и выше.	7.4. In the presence of the members of the Conciliation Commission, the Bank is obliged to install an operating system Windows 7 and higher as well as ES verification cryptographic program: • For *ICB* Subsystem – this is ES verification program provided by its manufacturer CJS INIST specified in paragraph 1.10 of this Procedure; • For «Direct integration» Subsystem – this is program CryptoPro CSP of version 4.0 and higher.
7.4.1. Сторона, отстаивающая подлинность спорного ЭД, обязана предоставить спорный ЭД, действовавшие в момент создания спорного ЭД Сертификаты ключей Стороны, подписавшей спорный ЭД, Банк обязан	7.4.1. The Party which upholds the authenticity of a disputed ED is obliged to provide the arguable document, the key certificates of the Party, which signed the disputed document, effective as at the date of generation thereof, and the Bank is

предоставить сами Ключи проверки электронной подписи, записанные на съемном носителе в виде файлов в формате, применяемом Системой (в случае если Клиент не предоставляет спорный ЭД, он предоставляется Банком).	obliged to submit the ES verification keys properly recorded on a removable media on files in the format accepted by the System (in case the Client fails to submit an arguable electronic document, the Bank is obliged to furnish such document).
7.4.2. Стороны обязаны предоставить все имеющиеся в их распоряжении Сертификаты ключей, информацию о проведенных плановых и внеплановых сменах Комплекта ключей Сторон и документы, удостоверяющие факты смены Комплекта ключей. Стороны также обязаны предоставить служебные ЭД Системы, в которых указаны факты получения ЭД из каналов связи и результаты их обработки (проверки).	7.4.2. Both Parties are obliged to submit all available key certificates, information regarding scheduled and unscheduled replacements of sets of keys and the documents which certify the fact of replacement of sets of keys. The Parties are also obliged to provide internal electronic documents of the System, which contain reference to receipt of ED via communication channels and results of their processing (verification).
7.5. Средством подтверждения ЭП являются: • Для Подсистемы «ИКБ» Ключи проверки электронной подписи, содержащиеся в Сертификатах ключей, с соответствующими Ключами проверки электронной подписи; • Для Подсистемы «Прямая интеграция» Сертификаты ключей.	7.5. ES verification keys are: • the Keys for verifying the electronic signature contained in the Key Certificated, with the corresponding Keys for verifying the electronic signature for «ICB» Subsystem; • Key Certificates for «Direct Integration» Subsystem.
7.6. Члены Согласительной комиссии должны выполнить следующие действия:	7.6. The Conciliation Commission members are obliged to carry out the following steps:
7.6.1. Произвести с помощью программы криптограческой проверки ЭП и средства подтверждения ЭП, использованного при подписании спорного ЭД, операцию проверки ЭП;	7.6.1. To perform verification of ES with use of the ES verification cryptographic software and ES verification keys utilized in the course of signing of the disputed ED;
7.6.2. Создать Протокол установления подлинности ЭД – документ на бумажном носителе, создаваемый Системой в качестве результата проверки ЭП спорного ЭД (далее - Протокол). Протокол должен содержать распечатанные на бумажном носителе Ключи проверки электронной подписи, использованные для установления подлинности ЭП, и заключение об итогах проверки ЭП спорного ЭД. Протокол должен быть подписан собственноручно всеми членами Согласительной комиссии;	7.6.2. To generate a Protocol of ED verification on paper media created by the System as a result of verification of ES of the arguable document (hereinafter referred to as the Protocol). The Protocol is to carry electronic signature verification keys printed out on paper media employed for ES authentication, as well as to submit findings on verification of the disputed ED. The Protocol is to be signed in hand by all members of the Conciliation Commission;
7.6.3. Сравнить Ключи проверки электронной подписи, содержащиеся в Сертификатах ключей, с соответствующими	7.6.3. To compare the ES verification keys contained in the Key Certificates with relevant ES verification keys specified in the Protocol on

Ключами проверки электронной подписи, зафиксированными в Протоколе установления подлинности ЭП спорного ЭД, и установить, тождественны ли они, внести об этом запись в Протокол (данная запись заверяется подписями членов Согласительной комиссии);	authentication of ES of the arguable ED, as well as determine their identity, make a relevant record in the Protocol (such record is to be certified by the signatures of the members of the Conciliation Commission);
7.6.4. Установить, являлись ли Ключи проверки электронной подписи действующими на момент выработки ЭП спорного ЭД, и внести запись об этом в Протокол (данная запись заверяется подписями членов Согласительной комиссии). Ключ проверки электронной подписи признается действующим на момент создания ЭП спорного ЭД в случае, если дата создания спорного ЭД приходится на период действия Ключа проверки электронной подписи. В противном случае Ключ проверки электронной подписи признается недействующим на момент создания ЭП.	7.6.4. To determine whether the electronic signature verification keys were effective as at the time of generation of the disputed electronic document, and make a relevant record in the Protocol (such record is to be certified by the signatures of the members of the Conciliation Commission). An ES verification key is deemed effective as at the date of generation of ES of the disputed electronic document, provided that the date of creation of the disputed document falls within the period of the effect of the ES verification key, failing which the ES verification key is to be deemed invalid as at the time of ES generation.
7.7. Согласительная комиссия признает ЭД подлинным, если одновременно выполнены условия: Ключи проверки электронной подписи в Сертификатах ключей и в Протоколе совпадают, Все результаты проверки ЭП в Протоколе положительны, Согласительная комиссия признала все Ключи проверки электронной подписи, содержащиеся в Протоколе, действующими на момент выработки ЭП. В противном случае Согласительная комиссия признает ЭД недействительным.	7.7. The Conciliation Commission will recognize ED as authentic, provided all of the following conditions are met simultaneously: ES verification keys specified in the Key Certificates and the Protocol are identical, All findings on ES verification recorded in the Protocol are positive, The Conciliation Commission recognized all ES verification keys listed in the Protocol as valid as at the time of ES generation. Elsewise the Conciliation Commission is to hold the electronic document invalid.
7.7.1. Средства подтверждения ЭП совпадают с соответствующими средствами подтверждения ЭП, зафиксированными в Протоколе.	7.7.1. ES verification keys coincide with corresponding means of ES verification keys, fixed in the Protocol.
7.7.2. Все результаты проверки ЭП в Протоколе положительны.	7.7.2. All findings on ES verification recorded in the Protocol are positive.
7.7.3. Согласительная комиссия признала все средства подтверждения ЭП, содержащиеся в Протоколе, действующими на момент выработки ЭП.	7.7.3. The Conciliation Commission recognized all ES verification keys listed in the Protocol as valid as at the time of ES generation